

RSA ClearTrust Ready Implementation Guide for Portal Servers and Web-Based Applications

Last Modified March 15, 2005

1. Partner Information

Partner Name	IBM Corporation
Web Site	www.ibm.com
Product Name	IBM Lotus Team Workplace
Version & Platform	6.5.1, Windows 2003 Enterprise
Product Description	IBM Lotus Team Workplace (QuickPlace) is a business-ready, self- service work space expressly designed for team collaboration. With Lotus Team Workplace, users can instantly create secure work spaces on the Web, providing them with a "Place" to coordinate, collaborate and communicate on any project or ad hoc initiative.
Product Category	Internet / Intranet



2. Contact Information

	Sales contact	Support Contact
Phone	800-IBM-4YOU	800-IBM-SERV
Web	www.lotus.com/products	www.ibm.com/software/lotus/support

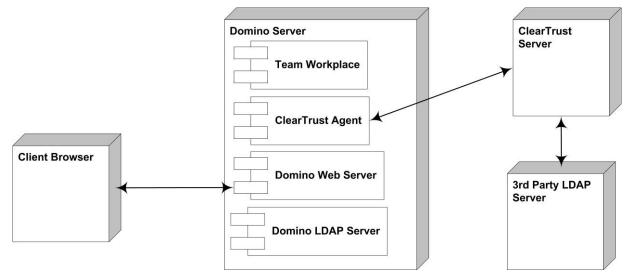


3. Solution Summary

Feature	Details
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	Νο
API-level Authorization Support (RuntimeAPI)	Νο
User Management (AdminAPI)	Νο

4. Integration Overview

To achieve single-sign-on with Lotus Team Workplace, the RSA ClearTrust Agent for Domino is installed on the Domino server. The agent is then configured to protect all Team Workplace pages, as well as any other desired pages. The Domino server is configured for multi-server single-sign-on, and authentication enabled. After this, users authenticated via either a ClearTrust authentication mechanism, or Domino's internal authentication, will be able to access all protected Domino assets.





5. Product Requirements

Hardware requirements

Component Name: Lotus Domino			
Memory	256Mb		
Hard Drive	1Gb (1.5Gb recommended)		

Software requirements

Component Name: Lotus Domino			
Operating System	Version (Patch-level)		
AIX	5.1, 5.2		
OS/400	VSR1, VSR2, i5OS VSR3		
Windows 2000	Server, Advanced Server		
Windows 2003	Server, Enterprise		
Solaris	8,9		
Red Hat Enterprise Linux	2.1		

Component Name: Lotus Team Workplace			
Operating System	Version (Patch-level)		
AIX	5.1, 5.2		
OS/400	VSR1, VSR2, i5OS VSR3		
Windows 2000	Server, Advanced Server		
Windows 2003	Server, Enterprise		
Solaris	8, 9		

Component Name: RSA ClearTrust Agent for Domino			
Operating System Version (Patch-level)			
AIX	5.1, 5.2		
Windows 2003	Server		
Domino	6.5.1IF1		



6. Product Configuration

This section provides instructions for integrating the partners' product with RSA ClearTrust. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components, including the ClearTrust servers and Entitlements Manager, need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

In order to achieve this integration, the following steps are necessary:

- Install & Configure Domino Server
- Install & Configure RSA ClearTrust Agent for Domino
- Install & Configure Lotus Team Workplace

Installation & Configuration of the Domino Server

Using the Domino 6.5.1 installation media, start the setup program. During the setup process, customize as necessary for your requirements, but be sure to choose to install the **Domain Enterprise Server**.

After the installation of the base server, install the Interim FixPack 1. Lotus Team Workplace (LTWP) requires Domino 6.5.1 IF1. Also, if you do not already have a Domino Administrator client already installed, you should install one at this time.

Configuration

Once the basic server and IF1 are installed, start the Domino server. When you start it for the first time, you will be prompted to configure the server. Unless you have a pre-existing Domino installation that you are integrating this server into, select the stand-alone server option.

During the setup process, if you save an external copy of the administrator's id file, it will be easier to find from the client.



Server	setup				X	
	Specify	an Administrator name and	password		Lotus software	
	can use	te the Administrator's ID, you e the name of a specific perso o be used by several people.				
	ŶО	First name:	Middle:	Last name (or generic acc admin	ount name):	
	~ 0	Administrator password:		Confirm password:		
		Minimum of 5 characters The Administrator ID file will be stored inside the server's Domino Directory.				
		Also save a local copy of C:\Lotus\Domino\Data\a			Browse	
	_	L I want to use an existing C:\Lotus\Domino\Data\a		ID file:	Browse	
Ŀ	lelp			< <u>B</u> ack <u>N</u> ext >	Cancel	

Also, be sure to select the **Web Browsers (HTTP services)** option, since it is not selected by default.

Server	' setup	X
	What Internet services should this Domino Server provide?	otus software
	Select the Internet services this Domino server will provide. Basic Notes and Domino ser are set up by default. (You can always change these options later in the Domino Director	
	Setup Internet services for: Web Browsers (HTTP services) Internet Mail Clients (SMTP, POP3 and IMAP services) Directory services (LDAP services)	
	To customize all other Domino services, click Customize.	mize
H	Help < Back Next > Ca	ancel

After this configuration process ends, start your Domino server, and ensure that it starts up correctly. You should also use the admin.id file created above to enable you to administer the server from a Domino Administrator.



Installation & Configuration of the RSA ClearTrust Agent for Domino

Prior to beginning installation of the RSA ClearTrust Agent, stop the Domino server. Then, start the agent setup program. Ensure that the agent detects the correct installation directory for Domino.

Make sure that the SSL settings entered in this process match the settings in your RSA ClearTrust servers' configuration files. For more information, consult the RSA ClearTrust Agent for Domino's Installation & Configuration Guide.

During the installation procedure you will be prompted for the address of a Dispatcher server, and an Entitlements server. While the dispatcher's address is required, the Entitlements server's address is required only if it is not connected to a dispatch server.

Remember the web server name you enter during the setup, as you will need to enter the exact same name into the Entitlements manager.

Installation & Configuration of Lotus Team Workplace

To begin installation, stop the Domino server, and then run the LTWP setup program. Ensure that it detects the correct Domino installation directory. After the installation concludes, a setup program will run. During the configuration, you will be asked for credentials for an administration account.

Note: Ensure that this user name is unique among user names from any LDAP stores you will attach LTWP to. LTWP authenticates to a separate data store by default, and will not be able to distinguish between users if there is overlap.

Specify name and passw	ord	×
Lotus. software	Provide the name and password for the person who is going to administer this Lotus Team Workplace server: User name: Password: Verify password:	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Once LTWP is installed and configured, restart Domino, and ensure that it starts successfully. Next, Domino must be configured for multi-server single-sign-on according to the instructions in the Lotus Team Workplace Administrator's Guide.



Disable ClearTrust DSAPI Filter

Note: There is a known issue with authenticating via the QuickPlaceLoginForm while the agent is installed. While using RSA ClearTrust Agent v4.6 for Domino, authenticating a user via QuickPlaceLoginForm may cause the Domino server to exit. See <u>Known Issues</u> for more information.

Because of this issue, disable the RSA ClearTrust DSAPI filter for further configuration (it will be reenabled later). To do this, start the Domino Administrator, and open up the server document for the server you created for LTWP. Under Internet Protocols, on the HTTP tab, you will see the DSAPI section halfway down on the right hand side of the document. Remove the ct_domino65_agent.dll entry, but make note of it, as you will replace it later. Then restart the Domino server.

People & Groups Files Server Mess Server: ps116/ltwp Release 6.5.2 on Window		uration	Logout Preferences Hell
Server	To:	DSAPI	
Configurations	Disabled	DSAPI filter file names:	ndolextn nquickplace C:\DominoAgent4.6 \lib\ct_domino65_agent.dll
External Domain Network	Disabled	Exclude From	
Cleanup script file		Logging URLs:	





Once the server restarts, start configuring the LTWP installation.

- Create a Web SSO Configuration document, or add the LTWP server onto an existing one. When creating the SSO document, this guide used a Domino SSO Key.
- Create a mapping form to map authentication to the QuickPlaceLoginForm.
- Restart the server.
- 1. Use the Domino Administrator and open the hub server:
 - a. Select the Configuration tab.
 - b. In the navigation pane, choose Server.
 - c. Click the Web button, and select Create Web SSO Configuration.

PELAB Domain 🙍 Welcome 🗙							
People & Groups Files Server Me	essaging Replic	ation Configuration					
Server: peDev/rsaPE Release 6.5.3FP1 on Wi	indows NT 5.2			Use [Directory C	urrent Server	•
Server Current Server Document	Add Server	ØEdit Server (Add to Cluster	🖲 Delete Server	🛞 Web 🕶		
All Server Documents	Domain	Server ^		Title	<u>⊂</u> reate Virtu		F
Configurations	✓ peLab				Create URL	. Mapping/Redirection Protection	
Programs		peDevirsa	aPE	Partner Engineerin Server	Cre <u>a</u> te Rea		
📰 External Domain Network Inf				Jeivei	_	nt Configurations	_H
🕨 🛐 Messaging					Crea <u>t</u> e Wet	b SSO Configuration	
S Replication							

Note: If you have a mixed R5/D6 environment, you will need to use the **Create Web R5 (SSO configuration)** button found in the action bar of Server documents. If you have a pure D6 environment, you can use the method outlined here or use Internet Site documents. For more information, see the IBM Redbook.



- 2. In the SSO Configuration document, make the following entries
 - a. Select LtpaToken.
 - b. Leave the Organization field empty.
 - c. Select and add all of the servers from the directory to the Domino Server Names field (this uses the proper hierarchical name for each server).
 - d. Enter the Internet domain that all of your servers share (you should precede this name with a leading period; Domino 6 will insert it when the document is saved if you forget).

Web SSO Configuration for : LtpaToken	Serence -	S 1
Basics Comments Administration		
Token Configuration	Token Expiration	
Configuration Name: LtpaToken	Expiration (minutes):	300
Organization:	Idle Session Timeout:	🗖 Enabled
DNS Domain: .pe.rsa.net		
	_	
Participating Servers		
Domino Server Names: ps116/ltwp		

e. Select **Keys** from the action bar and click **Create Domino SSO Key**. You will receive a confirmation when it has been successfully created.

関 Save & Close	🖉 Keys 🔻 🛞 Cancel			
Web SSO	Create Domino SSO Key Import WebSphere LTPA Keys	paToken	2 State	10 m
Basics Comments	Administration			
Token Configura	ation		Token Expiration	
Configuration Nam	ie: [©] LtpaToken _		Expiration (minutes):	۳ 300 ي
Organization:	r _		Idle Session Timeout:	🗖 Enabled
DNS Domain:	[©] .pe.rsa.net_			
Participating Se				
Domino Server Na	mes: 『ps116/ltwp』💌			

f. Save and close the Web SSO document.

Note: The Web SSO document is automatically encrypted with the user's ID that created it. If another administrator subsequently needs to edit the document, the administrator will receive a warning about the document being encrypted and will not be able to edit it.

If this happens, delete the document and create a new one so that you can add all the servers to the document.



- 3. Open each Server document and make the following changes to the Internet Protocols Domino Web Engine tab:
 - a. Session authentication: Multiple Servers (SSO)
 - b. Web SSO Configuration: LtpaToken.
 - c. Then Click Save and Close.

LTWP Domain 🔣 Itwp's Directory - Server\Web 🗙					
People & Groups Files Server M	essaging Replication Configurat	ion			
Server: ps116/ltwp Release 6.5.2 on Wind	ows NT 5.2		Use Directo		
Server	Edit Server 🖓 Create W	'eb (R5) 🕄 Cancel			
Current Server Document		aad 565 5 6 56 5 5 5 5 5 5 5 5 5 5 5 5 5 5			
All Server Documents		n 10 * 11 m	A Comment of the second s		
Configurations	Server : ps116/ltwp	S' assiere States	**************************************		
Connections	and the second second second	. 0001666 A. 6x.x			
Programs	Basics Security Ports Ser	ver Tasks Internet Protocols	MTAs Miscellane		
🧱 External Domain Network In					
🕨 🛐 Messaging	HTTP Domino Web Engine	DIIOP LDAP			
S Replication					
III Directory	HTTP Sessions				
Policies	Session authentication:	Multiple Servers (SSO)			
🖉 🏡 Web	Web SSO Configuration:	LtpaToken			
💷 Web Server Configurations		Elparoken			

4. Open domcfg.nsf. If domcfg.nsf does not exist you will need to create it. See the Domino documentation for information on how to do this.

People & Groups Files Server Messaging Replication Configuration						
Server: ps116/Itwp Release 6.5.2 on Windows NT 5.2 Show me:				Databases only		
🤝 🗁 C:\Domino\Data		Title 🗘	Filename 🗘	Physical Path 🗘	File Format 🗘	Size 🗘 🔰 🛛
🕨 🧰 domino	\diamond	Administration Request:	admin4.nsf	C:\Domino\Data\adm	R6 (43:0)	2,161,152
Doc	\diamond	Java AgentRunner	agentrunner.ns [.]	C:\Domino\Data\Ager	R5 (41:0)	458,752
🚞 gtrhome		Bookmarks (6)	bookmark.nsf	C:\Domino\Data\bool	R6 (43:0)	7,340,032
🛅 help	۵.	Local free time info	busytime.nsf	C:\Domino\Data\busy	R6 (43:0)	393,216
🕨 🧰 iNotes	Ó.	Catalog (6)	catalog.nsf	C:\Domino\Data\cata	R6 (43:0)	1,898,496
🛅 mail	Ő.	Itwp's Certification Log	certlog.nsf	C:\Domino\Data\certl	R6 (43:0)	458,752
🛅 modems	Ő.	Server Certificate Admin	certsrv.nsf	C:\Domino\Data\certs	R6 (43:0)	1,331,712
MeetingArchive	Š.	Domino Directory Cache	dbdirman.nsf	C:\Domino\Data\dbdi	R6 (43:0)	746,496
PlaceCatalog.ft	Ś	Offline Services	doladmin.nsf	C:\Domino\Data\dola	R6 (43:0)	524,288
V C QuickPlace	Ő.	Domino Web Server Co	domcfg.nsf	C:\Domino\Data\dom	R6 (43:0)	944,640



- 5. Create a mapping form to map authentication to the QuickPlaceLoginForm.
 - a. Applies To: All Web Sites/Entire Server
 - b. Target Database: QuickPlace/resources.nsf
 - c. Target Form: QuickPlaceLoginForm
 - b. Then Click Save and Close.

LTWP Domain 👫 Sign In F	orm Mapping : All 🗙
🖫 Save & Close 🛛 🗙 Ca	ancel
'Sign In' Form	Mapping
Site Information	
Applies To:	All Web Sites/Entire Server
	C Specific Web Site/Virtual Server
Comment:	۲ ــــــــــــــــــــــــــــــــــــ
Form Mapping	
Target Database:	^ℤ QuickPlace/resources.nsf_
Target Form:	[©] QuickPlaceLoginForm _

- 6. Open the notes.ini file located in the Domino install directory and add the following parameter QuickPlaceUseDSAPIDNs=1
- 7. Restart both servers.





Point Team Workplace at Domino User Store

Open up LTWP home page in a browser, and login as the LTWP administrator created during installation. Under **Server Settings**, select **User Directory**, then **Change Directory**. Select Domino Server as the type, and point it at your Domino server. Then, select to disallow new users. Save your changes, and log out of LTWP. This is necessary so LTWP will pick up the Domino users.

User Directory - quickplac	e - Microsoft Internet Explorer	<u>- 0 ×</u>
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	Iools Help	R
Address 🙋 http://ps116.pe.rsa	a.net/QuickPlace/quickplace/Admin.nsf/cf07bfcad7af887a0525670800167221/b4ef119005fbd54a052567080016713b/?E	• 🔁 Go
Lotus. Team Workplace		IBM. ^
admin		-
	Change User Directory Back	Next
	You can specify a user directory from which place members can be selected.	
	Directory. You can specify a directory from which place managers can select members. Select the directory type and name below:	
	Type: Domino Server 💌	
	Warning: New installations should not use this directory type. Directory access usi the Domino NRPC protocol is supported for backward compatibility purposes only. You should convert to LDAP for directory access before you upgrade the external user name format in any of the places on this server. See the installation documentation for more information. Name: ps116.pe.rsa.net	1
	New Users. Do you want to allow place managers to create new users in each pla or require managers to select existing users only from the available directory?	ice,
	C Allow managers to create new users in each place.	
	C Disallow new users - Require managers to select existing users from the availabl directory.	le
	Back	Next
	Back	Next

By default, LTWP uses Cloudscape as its user repository. To ease the SSO process, it should be using only Domino users. By pointing LTWP at Domino, and not allowing new user creation, the only user in Cloudscape will be the LTWP administrator created during installation. The RSA ClearTrust repository, for the purposes of this implementation guide, will be kept separate from the Domino user repository, so those two will need to be separately synchronized.

Log back into LTWP as the LTWP administrator. This time, select **Security** under **Server Settings**. In the administrator section, click **Add**, and add a Domino user as LTWP administrator.

🗿 Security - quickplace - Mic	rosoft Internet Explorer	IX
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ols <u>H</u> elp	<i>.</i>
Lotus. Team Workplace		. ^
admin Sign Out	Back Next	
◆ Go Up		
Instructions	Server Security: Add Access	-
Security	Administrators. Provide membership information for those who are permitted to administer this server. Note that administrators have supreme power, including deleting places and PlaceTypes.	_
User Directory		
Other Options	Type the name of each individual or group to add on a new line, or click Directory to select names from the directory.	
Select Time Zone	admin/rsa	
Help	Clear All	
	Remember to enter each name on a new line!	
		~



Cleaning Up

Now, re-insert the ClearTrust DSAPI filter in the server document. Then, restart the server one last time.

Note: The RSA ClearTrust DSAPI filter should be the last filter in the list. Authentication will not behave correctly otherwise.

Testing the Setup

When Domino starts, you should be able to see startup notices for LTWP and RSA ClearTrust DSAPI filters. Note that the LTWP message will show up as QuickPlace.

🔞 ps116/ltwp: Lotus Domino Ser	ver 📃 🔍 🕺
02/09/2005 10:48:08 AM	
02/09/2005 10:48:08 AM	Mail Router started for domain LTWP —
02/09/2005 10:48:08 AM	Router: Internet SMTP host ps116 in domain pe.rsa.net
02/09/2005 10:48:09 AM	AMgr: Executive '1' started
02/09/2005 10:48:09 AM	LDÅP Schema: Finished loading —
02/09/2005 10:48:09 AM	JUM: Java Virtual Machine initialized.
02/09/2005 10:48:09 AM	HTTP Server: Java Virtual Machine loaded
02/09/2005 10:48:09 AM	HTTP Server: DSAPI Domino Off-Line Services HTTP extensi
on Loaded successfully	
02/09/2005 10:48:09 AM	HTTP Server: DSAPI QuickPlace DSAPI Filter Loaded succes
sfully	
02/09/2005 10:48:09 AM	SchedMgr: Done validating Schedule Database
02/09/2005 10:48:10 AM	HTTP Server: DSAPI/ClearTrust Agent 4.6 Yor Domino 6.5 L
oaded successfully	
02/09/2005 10:48:10 AM	Servlet engine initialization was successful
02/09/2005 10:48:10 AM	LDAP Server: Started
02/09/2005 10:48:10 AM	HTTP JUM: File or directory C:\Domino\Data\domino\servle
t does not exist	1
02/09/2005 10:48:10 AM	QuickFlace: Successfully loaded Web SSO Configuration.
02/09/2005 10:48:11 AM	QuickPlace Server started. 350172.00
02/09/2005 10:48:12 AM	WITP Server: Started
>	V

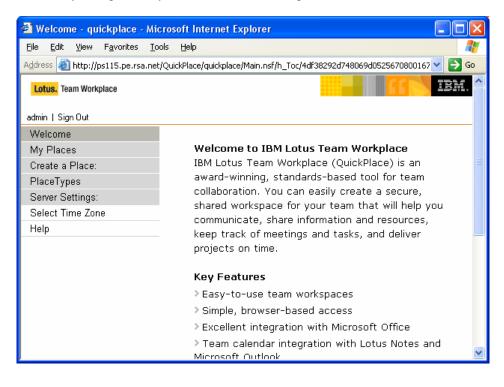
Using the RSA ClearTrust Entitlements Manager, create entries for the Domino server, and a sample Domino user. Then define resources for */homepage.nsf*, and */QuickPlace* on that server, and entitlements for your sample user. Remember that in Domino, you must protect the database and views separately (e.g. /abc, and /abc/*). Finally, add entitlements for the sample user for the Domino server resources.



From a new browser, browse to <u>http://servername.domainname</u>. You should see the Domino homepage. Then go to /homepage.nsf, which should show you the same page, after authentication via RSA ClearTrust.



When you navigate from there to the QuickPlace home page (/QuickPlace), you can see that you are automatically recognized by the RSA ClearTrust agent.





As a last check, navigate to the web administration database (/webadmin.nsf). You will Notice that even though the web admin database is protected by Domino, and not by RSA ClearTrust, the Domino agent supplies the credentials to Domino's native authentication, and the user is recognized from his RSA ClearTrust SSO cookie.

🕘 ps115/rsa@rs	a Administration - N	Microsoft Internet Explorer		
<u>File E</u> dit <u>V</u> iew	F <u>a</u> vorites <u>T</u> ools <u>H</u> e	elp		-
Address 🙆 http://	os115.pe.rsa.net/webad	min.nsf	~ 🖯	Go
People & Gr	oups] Files] Server]	Messaging Replication Configuration	<u>Preferences</u>	ΠHε
	You (admin/rsa) are or Server name: Host name: Version and build: Operating system: Directory & partition: Server date & time: Elapsed up-time: Transactions/minute: Peak # of sessions: Transactions: Waiting tasks: Availability Index: Mail domain: Mail domain: Mail tracking: Mail journalling: Shared mail:			



7. Certification Checklist for Portal Servers and Web-Based Apps

Date Tested: February 7, 2005

Product	Tested Version
RSA ClearTrust	5.5.2, 5.5.3
Team Workplace	6.5.1
Domino	6.5.1IF1, 6.5.2, 6.5.3
ClearTrust Agent for Domino	4.6

Test Case	Result
Product Characteristics for SSO Support Application/Portal is web-based, and supports access by a standard HTTP-based browser Application/Portal runs on Web Server Platform supported by RSA ClearTrust Application/Portal login interface can be modified or replaced Application/Portal can extract user information from RSA ClearTrust session cookie Application/Portal can extract user information from HTTP Headers	P P P P N/A
Application/Portal can extract authentication type from RSA ClearTrust session cookie Application/Portal can extract authentication type from HTTP Headers Application/Portal can perform SSO with other RSA ClearTrust-supported Web Server	N/A N/A P
HTTP basic authentication Forms based Forms based w/ URI retention	P P P
Login – Basic Authentication Access Denied for unauthorized user Successful login for authorized user Successful recognition of identity/personalization in 3 rd Party Product Successful recognition of identity/personalization after SSO with other RSA ClearTrust- supported Web Server	P P P P
Login –Graded Authentication Access Denied for unauthorized user Successful login for authorized user Successful recognition of identity/personalization in 3 rd Party Product Successful recognition of identity/personalization after SSO with other RSA ClearTrust- supported Web Server	N/A N/A N/A N/A

SWA/ATB

P=Pass or Yes F=Fail N/A=Non-available function



8. Known Issues

Authentication Via QuickPlaceLoginForm May Cause Domino Server Exit

While using RSA ClearTrust Agent v4.6 for Domino, authenticating a user via QuickPlaceLoginForm when the ClearTrust DSAPI filter is in place may cause the Domino server to exit. There is a fix available for this behavior from RSA technical support. To acquire this, ask for RSA ClearTrust Agent Hotfix 4.6.0.17.

This issue can also be worked around by deleting the login mapping created in the Web Configuration Database, and protecting the Team Workplace resources with ClearTrust.

